تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست)

The Effects of the Electronic War on the International Relations: A Study about the Electronic Attack on Iran (stuxnet virus)

غريب حكيم * **شرقي صبرينة**
فرقة البحث: التهديدات الإرهابية في الجوار الإقليمي وتداعياتها على الأمن الوطني الجزائري: الأبعاد واستراتيجية المواجهة
المدرسة الوطنية العليا للعلوم السياسية - الجزائر
gheriebhakim@hotmail.fr *mirouislem@yahoo.fr*

تاريخ الإرسال: 2020/02/06 * تاريخ القبول: 2020/03/29 * تاريخ النشر: 2020/06/01

ملخص:
تتناول هذه الدراسة موضوع تداعيات الحرب الإلكترونية على العلاقات الدولية، دراسة في النجوم الإلكتروني على إيران (فيروس ستكنست)، من خلال الوقوف على مفهوم الحرب الإلكترونية، ومدى تأثيرها على الامن الدولي والعلاقات الدولية، التي ساهمت في تطورها مجموعة من التحولات التكنولوجية التي شهده العالم في السنوات القليلة الماضية، فمع تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية، برزت العديد من الأنماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالا للصراعات المختلفة، سواء من قبل الفاعلين من الدول أو من غير الدول لحيازة أكبر قدر ممكن من النفوذ والتأثير السيبراني، حيث تهدف الدراسة إلى بيان مدى تأثير خطورة الحروب الإلكترونية على العلاقات الدولية، وتأتي أهمية الدراسة من خلال إثراء وتعميق البحث العلمي، وتوصلت الدراسة إلى أن الحروب الإلكترونية أصبحت تتعدى الحدود الوطنية، وسيصبح لها تأثيرا كبيرا على طبيعة العلاقات الدولية والسياسات العالمية، الأمر الذي أدى إلى صعود أدوار الفاعلين من الدول الصغيرة والمتوسطة، والفاعلين عن غير الدول على الساحة الدولية، كما ساعدت عوامل سهولة الاختراق الإلكتروني، وانخفاض تكلفة الهجوم والطبيعة غير المتماثلة للهجمات الإلكترونية وصعوبة اكتشاف الفاعل، وغياب أطر قانونية لتحديد العقوبات، على استخدام هذا الفضاء الجديد في شن هجومات إلكترونية مختلفة، تتراوح بين هجمات ذات طبيعة استراتيجية، وبين هجمات ذات أهداف عسكرية وأمنية، وأخرى ذات طبيعة سياسية.
الكلمات المفتاحية: الحرب الإلكترونية، الفضاء الإلكتروني، العلاقات الدولية.

Abstract:
This study deals with the effects of the electronic war on the international relationships. It studies specifically the electronic attack on Iran (stuxnet virus). It provides a definition of the electronic war and an account of its influence on the international security and the international relationships that have developed due to a number of technological changes the world witnessed in the few previous years. Multiple ways to use the electronic space came into existence due to its change into a space for international dealings. This is at the level of

* المؤلف المرسل

the uses with civil or military nature. This made the electronic space a field for the different conflicts by the countries or other activists to get as much dominance and the cyber influence. This study aims to explore the influence of the danger of the electronic war on the international relationships. The importance of this study lies in the fact that it enriches the scientific research. It comes to the conclusion that the electronic wars go beyond the national borders and it will have a great influence on the nature of the global relationships and the international politics. That led to the emergence of small and medium countries and other independent activists at the international scene. Also, many factors helped in the use of this new space in launching different electronic attacks which vary between strategic attacks, attacks with military and security ends, and others with a political nature. These factors include the easiness of the electronic penetration, the low cost of the attack, the non identical nature of the electronic attacks, the difficulty of finding the attacker, and the absence of law frames to determine the punishments.

Key Words: *the electronic war, the electronic space, the international security, the international relations*

مقدمة:

لم تعد المداخل النظرية السائدة في حقل العلاقات الدولية قادرة على استيعاب التحولات الاستثنائية التي تشهدها المواجهات العسكرية في الآونة الأخيرة، إذ تماهت الحدود الفاصلة بين حالتي الحرب والسلم، وتجاوزت الحروب المواجهات العسكرية التقليدية لتشمل توظيف أدوات اقتصادية واجتماعية وإعلامية وافتراضية، كما تعددت مصادر التهديدات عبر التقليدية، وتداخلت أدوار الفاعلين.

وتتسم بيئة التهديدات الراهنة بعدم وجود حدود فاصلة بين النطاقات الداخلية والإقليمية والدولية، إلا أن المحصلة النهائية لهذه التهديدات تؤدي إلى تصاعد مستويات الانكشافات الداخلية، مما يزيد من الضغوطات على المستوى الداخلي بصورة غير مسبوقة.

ولقد أدت هذه التحولات إلى صعود الحرب الإلكترونية التي تتسم بالغموض وعدم اليقين حول طبيعة المواجهات العسكرية، وصعود شبكات التحالفات بين الدول والفاعلين المسلحين من غير الدول، بالإضافة إلى صعود الاستراتيجيات الهجينة (Hybrid Strategies) والدمج بين تكتيكات الهجوم والدفاع والردع بصورة متزامنة، ويرتبط ذلك التغيير بطبيعة التهديدات التي لم تعد مقتصرة على تهديدات الغزو الخارجي بل أصبحت تتضمن تهديدات غير تقليدية مثل الاختراق الداخلي، الجريمة المنظمة العابرة للحدود، الجماعات الإرهابية.

ولا ينفصل التغير في طبيعة الحروب عن التحولات التكنولوجية السريعة التي أسهمت في ظهور تقنيات متقدمة في مجال التسليح وتطوير أدوات غير تقليدية يمكن توضيحها في اخضاع الخصوم، واختراق الدول داخليا، من خلال الحرب الإلكترونية.

كما عززت الجماعات الإرهابية تحالفاتها البراجماتية مع الفواعل المسلحة الأخرى، مثل عصابات الجريمة المنظمة وشبكات تهريب المخدرات والأسلحة والميليشيات المسلحة، واستخدامهم للفضاء الإلكتروني مما أدى إلى ظهور مصطلحات جديدة مثل: الجماعات المرتزقة السيبرانية، المليشيات السيبرانية، والقراصنة السيبرانيون، والحروب السيبرانية أو الإلكترونية، والإرهاب الإلكتروني، ولهذا فقد أحدث ظهور الحروب الإلكترونية وبشكل فعلي على الساحة الأمنية والمعلوماتية منذ منتصف العقد الأول من القرن الحالي نقلة نوعية في مفهوم الحروب التقليدية من حيث الوسائل والأهداف والنتائج أيضا.

وفي هذا السياق تبلورت ظاهرة الحروب الإلكترونية التي اتسمت بخصائص مختلفة عن نظيرتها التقليدية، من حيث طبيعة الأنشطة العدائية، والفواعل والتأثيرات في بنية العلاقات الدولية، واعتمدت هذه الحروب على نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات.

في هذا الاطار سنحاول تناول الجدل السائد حول مفهوم الحرب الإلكترونية، وأنماط الحروب الإلكترونية، كما ستتطرق أيضا إلى دراسة الفاعلين الأساسيين للحروب الإلكترونية، سواء كانوا هؤلاء الفاعلين دولا أو من غير الدول، ثم تتناول الدراسة تداعيات ومخاطر الحروب الإلكترونية على العلاقات الدولية، وأخيرا سنحاول دراسة حالة في الهجوم الإلكتروني على إيران (فيروس ستكنست).

أهمية الدراسة:

تبرز أهمية الدراسة من حيث المكانة التي بات يحتلها مجال الفضاء الإلكتروني بين دول العالم، حيث أصبح هذا الفضاء مجالا مستهدفا بشكل كبير، وخصوصا مع ارتفاع وتيرة التقدم التكنولوجي والتقني والإلكتروني، والذي أعطى الإمكانية لضرب أي دولة أو منظمة في وقت قصير وتكلفة قليلة، وذلك باستخدام الإنترنت ووسائل الاتصال الإلكتروني الأخرى، الأمر الذي أدى إلى بروز تداعيات عديدة على العلاقات الدولية.

الاشكالية:

لم تعد الحرب في الوقت الراهن مجرد حرب تقليدية واضحة المعالم والأدوات، وإنما باتت خليطا من توظيف كافة الأدوات المتاحة، التقليدية وغير التقليدية، في ظل تحوّل تكنولوجي هائل يغير كثيرا من المفاهيم السائدة عن الحرب والصراع والردع، بحيث أضحى الملمح والهدف الجوهري هو "التفجير من الداخل " باعتباره الوسيلة الأمثل لهزيمة الخصوم.

ومن هنا يمكن صياغة المشكلة البحثية في سؤال رئيسي متمثل في: " ما هو دور وتأثير الحروب الإلكترونية على العلاقات الدولية ؟".

1. **<u>الحرب الإلكترونية جدلية المفهوم:</u>**

تحولت الساحة الإلكترونية العالمية إلى أرض معارك حقيقة في عالم افتراضي تقني يعتمد على كل ما هو جديد من صيحات التكنولوجيا الرقمية والاتصالية الحديثة، تعددت أشكال هذه الحروب ما بين الفردي والجماعي، والدولي والمؤسساتي، والسياسي والاقتصادي والاجتماعي، وغيرها من أشكال الحروب الدائرة عبر الفضاء الإلكتروني والبعيدة عن أنظار ومسامع البشرية، وانعدام وجود إطار ناظم للأنشطة التي تمارس من خلالها، فالحرب الإلكترونية بإعتبارها إحدى مجالات الحرب حديثة الطرح والتطور على الساحة الأمنية والمعلوماتية، تحتاج إلى جهود عديدة للضبط المفاهيمي، لا سيما أنه لا يوجد اتفاق بين المتخصصين والأكاديميين حول تعريف الحرب الإلكترونية.

توصف الحرب بأنها: " استمرار للسياسة، ولكن بأدوات أخرى ". فوفقا لكارل فون فلاوزفيتش لا تعد الحرب كونها مجرد أداة لتحقيق هدف محدد، وهو إجبار العدو على الإنصياع، لإدارة الدولة وفرض السلام وفق الشروط التي تحقق مصالح الطرف المنتصر. (Amstrom, 2005 , p.4).

كما تعرف الحرب أيضا بأنها " نزاع بين الوحدات السياسية تستعمل فيه القوة المسلحة " (زيتون، 2006، ص. 138).

يشير القاموس الدولي حول الحرب الإلكترونية على أنها " حرب يتم شنها من خلال أجهزة الحاسوب وشبكة الإنترنت وهي تشمل إجراءات هجومية لإلحاق الضرر بنظم المعلومات عند الخصوم، وأخرى دفاعية لحماية

النظم الخاصة بالمهاجمين، وقد تسبب الهجمات على هذه الأجهزة ضررا مساويا لما يسببه هجوم عسكري تقليدي " (الزهراني، 2017، ص. 236).

كما تعرف الحرب الإلكترونية بأنها: " حرب تخيلية أو افتراضية (Virtual Reality) ذات طبيعة غير ملموسة، تحاكي الواقع بشكل شبه تام، وهي حرب بلا دماء، بحيث تتلخص أدوات الصراع فيها بالمواجهات الإلكترونية، والبرمجيات التقنية، وجنود من برامج التخريب، وطلقات من لوحات المفاتيح ونقرات المبرمجين. " (جلعود، 2013، ص. 81).

وهناك من يربط الحرب الإلكترونية ببيئة الإنترنت فقط، كونها ساعدت على انتشار المعلومات في مختلف أرجاء المعمورة بشكل كثيف، وسهلت الوصول إليها بشكل سريع، بحيث يتم تعريف الحرب الإلكترونية بناءا على ذلك بأنها " الحرب التي تستهدف المعلومات وهي تعبير عن الإعتداءات التي تطال مواقع البيانات الموجودة على الإنترنت، وتحاول الاستيلاء على معطياتها، بين أطراف متناقضة الأهداف، ومتعارضة المصالح، ومختلفة المواقف " (جعفر، 2010، ص ص. 65-66).

ويشير هذا المفهوم إلى الأبعاد السياسية والعسكرية التي تتخذ من الفضاء الإلكتروني مسرحا لتنفيذ أجندتها وأهدافها، بحيث تستخدم تكنولوجيا المعلومات لإنجاز التفوق المعلوماتي، وحماية الخطط الاستراتيجية، والبقاء بعيدا عن دائرة الإصابة الإلكترونية (جعفر، ص. 66).

كما يشير مصطلح الحرب الإلكترونية إلى اعتداء رقمي منسق على نطاق واسع على حكومة من قبل حكومة أخرى، أو بواسطة مجموعات كبيرة من المواطنين،وهي إجراء تقوم به دولة قومية لاختراق أجهزة كمبيوتر وشبكات دولة أخرى لأغراض التسبب في ضرر، ويضيف أنه يمكن استخدام مصطلح الحرب الإلكترونية لوصف الهجمات بين الشركات.

تعتمد الحرب الإلكترونية الناجحة على شيئين: الوسيلة والضعف: الوسائل هي الأشخاص والأدوات والأسلحة الإلكترونية المتاحة للمهاجم، الضعف هو مدى استخدام اقتصاد العدو والجيش للإنترنت والشبكات بشكل عام (Dunnigan, 2002, p.11).

تعرف وزارة الدفاع الأمريكية الحرب الإلكترونية بأنها " استخدام أجهزة الكمبيوتر والإنترنت لإجراء الحرب في الفضاء الإلكتروني" (Michael, 2010, p.1).

وقد اجتهد عدد من الخبراء من ضمن اختصاصاتهم في تقديم تعريف يحيط بهذا المفهوم، فعرّف كل من " ريتشارد كلارك وروبرت كناكي" في كتابهما الشهير " حرب الفضاء الإلكتروني " على أنها " أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها ". (Clarke and, Knake, 2010, p. 15).

ويبرز في هذا التعريف السمات العسكرية والسياسية والاقتصادية للفضاء الإلكتروني المرتكز على عالم الاتصالات والمعلومات، وتطور وسائل التشبيك والتواصل، وعلى خلق أدوات تهديد مختلفة وخطيرة تقوم بإحداث أضرار ملموسة كبيرة ومدمرة، وهذا التدمير يتعدى حاجز الحاسوب بمراحل متقدمة، ومن أمثلة هذه الهجمات الهجوم الإلكتروني الروسي على تالين العاصمة الإستونية، العضو في حلف الناتو عام 2007 اثر خلافات سياسية، وكان هذا يعد أول هجوم دولي بمفهومه الإلكتروني، والذي قام بشلل البنى التحتية الحرجة في استونيا لمدة 3 أسابيع، الأمر الذي أدى إلى تدخل حلف الناتو في استونيا لتأمين الفضاء الإلكتروني، وتكرر الهجوم وأضراره البالغة على جورجيا من قبل روسيا عام 2008 (Clarke and, Knake, p.15).

يرى بعض القانونيين أن ديناميكيات عمل الحروب الإلكترونية تتقارب من ناحية قانونية مع إشاعة الرعب والإرهاب لذلك يمكن تعريف الحروب الإلكترونية استنادا لهذه النظرة القانونية بأنها " نظام قائم على الرعب المنتشر في الشبكة العنكبوتية (الإنترنت)، والتي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول، وإرهاقهم اقتصاديا، وإدخالهم في أزماتٍ نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت (Terror Silent) (عياد، 2007، ص. 65).

كما تعرف الحروب الإلكترونية أنها " الحروب التي تتم بالتعاون مع الحرب العسكرية، إذ أنها تصوب نيرانها نحو الأهداف الإلكترونية والرقمية والمعلوماتية، كالتجسس على الإشارات الصادرة من الأجهزة الحاسوبية التابعة للفئات المستهدفة " (بدران، 2010، ص. 30).

ويعتبر آخرون أن الحرب الإلكترونية هي امتدادا للحروب التقليدية والمادية، بحيث يتألف جندها من المدنيين والعسكريين في آنٍ واحدٍ، كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالا عدة، كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، وإحراج الساسة، والعبث بالمحتوى التقني والرقمي وغيرها.

يعرف حلف الناتو الحرب الإلكترونية على أنها " ذلك القسم العسكري الذي يستخدم إلكترونيات تهتم بالإجراءات التي تتخذ لمنع أو تقليل استخدام العدو لطاقته الكهرومغناطيسية المنبعثة الفعالة، والإجراءات التي تتخذ لحماية طاقتنا الكهرومغناطيسية المنبثقة الفعالة "(محمد البصيلي، 1989، ص. 31).

ويتضح مما تم عرضه من مفاهيم متعلقة بالحرب الإلكترونية بأن لها خمسة جوانب تحدد آلية عملها، أولها: أن هذه الحروب الرقمية تستهدف فئات معينة، قد تكون أفرادا، أو مؤسسات، أو منظمات، أو دول، وثانيها: أن بيئة المعلومات الرقمية هي المستهدفة في هذه الحرب، وثالثها: أن سلاح هذه الحرب هي النظم والوسائل الإلكترونية والاتصالية بشتى أنواعها، ورابعها: أن لهذه الحرب تكاليف سياسية واقتصادية واجتماعية وأمنية باهظة الثمن، أما آخر هذه الجوانب فهو الجوانب الأيديولوجي والذي قد يعتلي ممارسات هذه الحرب في الفضاء الإلكتروني. (جلعود، ص. 86).

ومن المتوقع أن تصبح الحرب الإلكترونية نموذجًا تسعى إليه العديد من الجهات نظرًا للخصائص العديدة التي تنطوي عليها، ومنها: (Lynn, 2010, p.98)

- **حروب لا تناظرية**: إن حروب الإنترنت هي حروب لا تناظرية حيث إن تكلفة الأدوات اللازمة لشن هكذا حروب هي تكاليف بسيطة مقارنة بتكاليف الحروب التقليدية، كما أنه لا تحتاج لدولة أخرى تقوم بتصنيع أسلحة مكلفة جدا مثل حاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة أخرى.
- **تمتع المهاجم بأفضلية واضحة:** في حروب الإنترنيت يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، وفي بيئة مماثلة يتمتّع بها المهاجم بأفضليّة، من الصعب جدا على عقلية التحصّن لوحدها أن تنجح، فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق وبالتالي المزيد من الضغط (عبد الغفار، 2016، ص. 11).
- **فشل نماذج الردع:** يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الإنترنيت، فالردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على هذه الحروب، فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل

ومن المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي، بعض الحالات قد تتطلب أشهرا لرصدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها (عبد الوهاب، 2017، ص. 21).

- **تعدي المخاطر الأهداف العسكرية:** لا ينحصر إطار حروب الإنترنيت باستهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة في البلدان المستهدفة، وهو أمر أصبح واقعيا في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادّية حقيقية تؤدي إلى انفجارات أو دمار هائل (عبد الغفار، ص. 12).
- **حرب رقمية:** وهي حرب تقنية متطورة، جسدت قمة التطور الذي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية التي شكلت بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيس لها فكانت نتيجة لذلك عرضة للتطور المستمر والتنوع والابتكار في تقنياتها ووسائلها لإرتباطها الرأسي بقمتي الهرم التقني للحضارة ألإنسانية، والمصالح الحيوية للدول (أحمد، 2013، ص. 47).

2. أنماط الحرب الإلكترونية:

يمكن طرح عدة أنماط لهذه الحروب من حيث مدي درجة شدة الصراع من عدمه، ومن أبرزها:

1.2. النمط الأول: الحرب السيبرانية الباردة منخفضة الشدة: حيث يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويعبر هذا النمط عن صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة ممتدة، ودائمة النشاط العدائي أو غير السلمي، بخلاف أنه عميق الجذور ومتداخل، وله نواح متعددة ثقافية، أو اقتصادية، أو اجتماعية، وعادة ما يتم اللجوء إلى القوة الناعمة للحروب السيبرانية في مثل صراعات كهذه، وإن كانت لا تتطور بالضرورة إلى استخدام القوة المسلحة بشكلها التقليدي، أو شن حرب إلكترونية واسعة النطاق (http://alimbaratur.com/?p=2850).

ولهذه الحرب السيبرانية الباردة وسائل عدة، منها شن الحروب النفسية، والاختراقات المتعددة، والتجسس، وسرقة المعلومات، وشن حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية، وتجلى هذا النمط في حالات الحروب في الصراعات السياسية، ذات البعد الاجتماعي – الديني الممتد، مثل الصراع العربي – الإسرائيلي، أو الصراع الهندي – الباكستاني، أو الصراع بين الكوريتين الشمالية والجنوبية، وغيرها.

في مثل هذه الصراعات، تنشط جماعات دولية للقرصنة للتعبير عن مواقف سياسية، أو حقوقية، مثل جماعة " ويكيليكس"، و" أنونيموس"، وكذلك أيضا في حالات الأزمات الدولية، مثل التوتر بين استونيا وروسيا في عام 2007، وكذا الاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، أو ما بين طهران وواشنطن (Sanger, 2012, p. 188).

وقد تعرضت روسيا للاتهام بالقرصنة الإلكترونية في الانتخابات الأمريكية الأخيرة لدعم المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلينتون (Bieber, 2000, pp. 124-128)

2.2. النمط الثاني: نمط الحرب السيبرانية متوسطة الشدة: حيث يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة على الأرض، ويكون ذلك تعبيرا عن حدة الصراع القائم بين الأطراف، كما قد يمهد لعمل عسكري، هنا تدور حروب الفضاء الإلكتروني عن طريق اختراق المواقع الإلكترونية، وتخريبها، وشن حرب نفسية ضد الخصوم، وغيرها.

يستمد هذا النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، خاصة في ظل بعض التقديرات التي تشير إلى أن تكلفة هذه الحروب قد تصل إلى أقل من 4 مرات من إنفاق نظيراتها التقليدية، بما يمكن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابة، وتاريخيا تم استخدام الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو في عام 1999 على يوغوسلافيا، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم. (http://alimbaratur.com/?p=2850).

أيضا برزت خلال الحرب بين حزب الله وإسرائيل في عام 2006، وكذلك بين روسيا وجورجيا في عام 2008، والمواجهات بين حماس وإسرائيل في عامي 2008 و2012.

3.2. النمط الثالث: الحرب السيبرانية الساخنة مرتفعة الشدة: حيث يعبر ذلك النمط عن نشوء حروب في الفضاء الإلكتروني منفردة، وغير متوازية مع الأعمال العسكرية التقليدية، ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجيا، واتساع الاعتماد بين الدول والفواعل من غير الدول على الفضاء الإلكتروني.

ينطوي هذا النمط من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار، وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني، والاستحواذ على القوة الإلكترونية.

3- <u>الفواعل في الفضاء الإلكتروني:</u>

خلافا للحروب التقليدية التي سيطرت على الحروب ين الدول لفترات طويلة من الزمن، فإن الحروب الإلكترونية تأتي في ظل ساحات مفتوحة تتسع لجميع الفاعلين من الدول وغيرها، وذلك نتيجة سهولة دخول ساحة الفضاء الإلكتروني، وعدم اقتصار امتلاك الأسلحة الإلكترونية على دول أو جهات بعينها، وتتكون تركيبة الفواعل في الفضاء الإلكتروني من مستويين، الأول على المستوى الدولاتي، أمَا الثاني فهو على المستوى اللادولاتي (بلفرد،2016، ص. 153).

1.3. الفواعل الدولاتية: وهنا نُشير أساسا إلى الاحتكار القانوني والمُنظم للدولة للفضاء الإلكتروني، من خلال مختلف أجهزتها(وزارات، وحدات الأمن...)، حيث تعتبر الدولة فاعل محوري في تسيير الفضاء الإلكتروني انطلاقا من إمكاناتها المادية والبنيوية والبشرية والقانونية، ولذلك لابد للدولة من التحكم في مجال الفضاء السيبراني، وهو الفضاء الذي يزاحمها فيه العديد من الفواعل الأخرى، التي قد تصل حد تهديد مصالح الدولة نفسها.

وقد أوضح تقرير مؤسسة Control Risks _ وهي إحدى المؤسسات العالمية المستقلة في مجال استشارات المخاطر السياسية والأمنية – أن نسبة الزيادة في أعداد الهجمات السيبرانية ذات الدوافع السياسية خلال عام 2015 بلغت 56% ، وتوقع التقرير أن أعداد الدول القومية القادرة على شن الهجمات الإلكترونية ذات التأثير الشديد خلال عام 2016 بلغت حوالي 45 دولة مقارنة بحوالي 10 دول فقط مقارنة بعام 2014.

وتتشكل القدرات الدفاعية والهجومية الإلكترونية للدول في أغلب الأحيان من الجنود والمحاربين السيبرانيين: (عبد العزيز، 2017، ص. 13).

- **الجنود الإلكترونيون:** وهم جنود متخصصون في مجال تكنولوجيا المعلومات يعملون في الأجهزة العسكرية للدول، ويشكلون ما يشبه الفصائل أو الوحدات العسكرية داخل الجيوش الوطنية للقيام بالهجمات الإلكترونية لصالح دعم الأهداف الاستراتيجية للدول في القيام بالهجمات الإلكترونية أو تشكيل حائط للدفاع عنها ضد الهجمات الإلكترونية.

- **المحاربون الإلكترونيون:** هم عملاء سريون للدول يعملون على تطوير قدراتها في مجال الهجمات الإلكترونية والقيام بتلك الهجمات نيابة عنها، إلا أنهم قد يتمتعون بالاستقلالية في اختيار الهدف ووقت وآليات تنفيذ الهجوم.

2.3. الفواعل اللادولاتية: أتاح الفضاء السيبراني للفاعلين من غير الدول، مجالا جديدا أكثر فاعلية، يمكنهم من خلاله امتلاك القدرة على ممارسة القوة الصلبة والناعمة بدرجات مختلفة، وذلك بعيدا عن المجالات التقليدية لممارسة القوة على الساحة الدولية، وهنا يأتي دور الأفراد والجماعات ونشطاء القرصنة الإلكترونية والميليشيات السيبرانية اللذين أصبحوا بإمكانهم التحكم في توجهات الدول وإدارتها وفق سياسات معينة من خلال الفضاء السيبراني، وسنتناول أهم هذه الفواعل كالتالي:

- **الهاكرز الأفراد Individuel Hackers :** حيث أضحى الفرد فاعلا مهما في الفضاء السيبراني، حتى أنَه له القدرة على إحداث الثورة الرقمية، وتُصبح تلك الثورة مجال استخدام للدولة نفسها، وقد تلجأ بعض الدول أو المؤسسات غير الحكومية إلى الاستعانة بهؤلاء الهاكرز سواء بشكل رسمي من خلال ضمهم إلى الوحدات العسكرية والاستخباراتية.
- **نشطاء القرصنة الإلكترونية Cyber Hacktivist**: يطلق هؤلاء النشطاء الهجمات السيبرانية بشكل أساسي لتحقيق أهداف سياسية، حيث تشكل من منظورهم وسيلة للاحتجاج العام أو التعبير والدفاع عن الأيديولجية التي يؤمنون بها او طرح أجندة سياسية يرغبون في تبنيها.

ومن أبرز الأمثلة على نشطاء القراصنة نشطاء الأنونيمس الذين قاموا بشن العديد من الهجمات على عدد من الشركات العالمية مثل سوني، وماستر كارد وبعض المواقع الحكومية الأمريكية، وقاموا كذلك ببعض الهجمات الإلكترونية لدعم الثورات العربية.

- **المليشيات السيبرانية Cyber Militia:** هي فصائل أو وحدات تماثل المليشيات العسكرية، تضم مجموعات كبيرة العدد نسبيا، وتتطلب تحديد المهام بين أعضائها لتوزيع السلطة والمسؤوليات، وقد تأتي تلك المليشيات وفقا لثلاثة نماذج وهي (المنتدى، والخلية، والتسلل الهرمي) (عبد العزيز، ص. 14).
- **المجموعات الافتراضية Default groups:** وهنا يأتي دور القراصنة (Hackers)، وغالبا ما يسعون لتحقيق أهداف مختلفة (ربحية، سياسية، إيديولوجية...)، ومثال دلك نجد المجموعة الافتراضية المشهورة (Anonymous)، والتي تسعى لتسويق خطابات ومطالب سياسية في العالم (بلفرد، ص. 153).

4- تداعيات الحرب الإلكترونية على العلاقات الدولية

أضافت الحرب الإلكترونية مدخلا جديدا في العلاقات الدولية، خاصة في مجال الصراعات والحروب، حيث أصبح هناك نوع من الحرب الخفية التي تشنها الدول فيما بينها، وقد أدى اتساع علاقة الدول بالفضاء الإلكتروني، وما خلفته من حروب إلكترونية إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي:

1.4. تصاعد المخاطر الإلكترونية: زادت وتيرة تصاعد المخاطر الإلكترونية خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب (عبد الصادق، 2016، ص ص. 22- 26).

2.4. تعزيز القوة وانتشارها: فمن جهة عزز الفضاء الإلكتروني ما يسمي بـ "القوة المؤسسية" في السياسة الدولية، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في تشكيل السياسة

العالمية، ومن ثم فإن سهولة الحصول على تلك القوة السيبرانية أدت إلى ما يسمى بنشر القوة من خلال انتقال القوة من التركز في أيدي الدول الكبرى لتتوزع بين أكبر عدد من الفاعلين من الدول المتوسطة والصغيرة، وكذلك الفاعلين من غير الدول، وهو ما يعني ضعف سيطرة الدولة وارتفاع حجم التهديدات التي تواجه النظام الدولي، من خلال زيادة قدرة الفاعلين الأصغر في السياسة الدولية على ممارسة كل من القوة الصلبة والقوة الناعمة من خلال استغلال الفضاء السيبراني (عبد العزيز، ص. 16).

من جهة أخرى، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة. فبعدما كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولا، أم من غير الدول.

3.4. عسكرة الفضاء الإلكتروني: وذلك سعيا لدرء تهديداته على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة، وزيادة الانفاق على الأمن السيبراني في العديد من الدول، ومنها الولايات المتحدة الامريكية حيث خصصت وزارة الدفاع الأمريكية خلال الفترة من 2010 إلى 2015 حوالي 22 إلى 30% من ميزانيتها للأمن السيبراني، وتم تخصيص حوالي 19 مليار دولار للأمن السيبراني من قبل الولايات المتحدة الأمريكية خلال عام 2017.

4.4. إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول: وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.

5.4. تحديث القدرات الدفاعية والهجومية: حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية، ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، وهنا يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى (عبد الصادق، 2012، ص. 30).

6.4. توتر واحتقان العلاقات الدبلوماسية بين الدول: غالبا ما تسفر الهجمات السيبرانية عن إحداث نوع من التوتر والاحتقان في العلاقات الدبلوماسية بين الدول، وعلى سبيل المثال التوتر الذي حدث بين روسيا وأمريكا خلال الانتخابات الرئاسية الأمريكية.(عبد العزيز، ص. 17).

وفي هذا الصدد وبالاستناد إلى استطلاع الرأي الذي أجراه مركز أمريكي للدراسات " بيو للدراسات " (PWE) وشمل 26 دولة، وشمل الاستطلاع على عدد من الأسئلة بخصوص رأي الشعوب في قدرة حكوماتهم على التصدي لأي هجوم إلكتروني واسع يعرض معلومات الأمن القومي والبنية التحتية العامة ونتائج الانتخابات للخطر.

وكانت النتائج أن (74%) من الشعوب تعتقد أن الهجمات الإلكترونية من الممكن أن تؤثر على معلومات الأمن القومي الحساسة، و (21%) لا يعتقدون ذلك، و (69%) يعتقدون أن الهجمات الإلكترونية من الممكن أن تؤثر على البنية التحتية العامة للبلاد، و (25%) على خلاف ذلك، و (61%) يعتقدون أن الحروب الإلكترونية من

الممكن أن تؤثر في نتائج الانتخابات في بلدانهم، و(33%) لا يعتقدون ذلك (بدوي بريوش، 2018-2019، ص. 29).

من جهة أخرى فإن الحروب الإلكترونية تأتي في الصف الأول كأكبر التهديدات التي تؤثر على أمن وسلامة المعلومات، والبنى التحتية للدول، فقد أصبحت الحروب الإلكترونية من ضمن قائمة المخاطر المستهدفة للأمن العالمي والعلاقات الدولية، وفي هذا الصدد فقد أجرت شركة الحماية الروسية Kaspersky lab بالتعاون مع B2B International دراسة حول هذا الموضوع (https://www.tech-wd.com/wd/2012/09/08/kaspersky).

وشملت الدراسة والمسح أكثر من 3.300 خبير ومحترف في تقنية المعلومات وشملت الدراسة 22 دولة بما فيها دولتين من الشرق الأوسط هما السعودية والإمارات، جميع المشاركين على دراية بقضايا وسياسة أمن المعلومات إضافة إلى المعرفة الجيدة بخصوص المسائل الأمنية على الصعيد العالمي.

كما تم وضع المشاركين من الشركات والمؤسسات في ثلاثة مجموعات وبحسب الأحجام إلى: المؤسسات الصغيرة (S) ما بين 10-99 مقعد، المؤسسات المتوسطة (MB) مابين 100-999 مقعد، الشركات (E) أكثر من 1000 مقعد (https://www.tech-wd.com/wd/2012/09/08/kasperskyt).

وحسب هذه الدراسة يرى نصف الخبراء أن الحروب الإلكترونية أصبحت من بين أكبر ثلاثة مخاطر الأكثر تهديدا للأمن القومي والعلاقات الدولية، والتفسير الرئيسي لهذا هو أن الحروب الإلكترونية أصبحت أكثر المخاطر انتشارا اليوم وبالتالي لا يمكن إهمالها وغض النظر عنها.

5- دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست)

1.5. التعريف بالفيروس: فيروس "ستكسنت" Stuxnet وهو عبارة عن برنامج كمبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا، وعلى الرغم من أنه تم اكتشاف هذا الفيروس لأول مرة من قبل شركة بيلاروسية تدعى VirusBlockAda ، حيث قالت إنها عثرت على التطبيق الخبيث في جهاز كمبيوتر يعود لأحد عملائها الإيرانيين.

وهناك من يرى أن وكالَتي الاستخبارات الأمريكية والإسرائيلية استطاعتا تصميم هذا الفيروس والذي عمل على اختراق وتعطيل المنشآت النووية الإيرانية، (Rid, 2017, pp.80-81)، كما أن هناك من يرى أن إسرائيل قامت لوحدها بشن هذا الهجوم الإسرائيلي، حيث إن الهجوم كان دقيقًا إلى درجة تحديد عدد أجهزة الطرد المركزي، وقد احتاج تفعيل هذا الهجوم مجرد تشغيل أجهزة الكمبيوتر في المنشآت الإيرانية، وبمجرد أن تسلل الفيروس إلى الأجهزة أخفى وجوده واستطاع تعطيل أجهزة الطرد المركزي بمهارة فائقة، حيث عمل على تغيير الضغط داخل أجهزة الطرد المركزي، وجعل سرعة الدورات داخل الأجهزة متفاوتة، مما أدى إلى انهيارها.

ويعتبر البعض أن نجاح هذا الهجوم انتقل بالعالم إلى مرحلة توظيف الهجمات السيبرانية في تحقيق أضرار مادية متعمدة، وهو ما يفتح الباب أمام الكثير من التكهنات بأن مثل هذه الأسلحة المتطورة يمكن أن تصبح أمرًا شائعًا في المستقبل.

ففي 25 سبتمبر 2010، أكدت إيران أن العديد من وحداتها الصناعية تعرضت لهجوم إلكتروني بعد إصابتها بفيروس "ستكسنت" ويعد هذا الفيروس وفق العديد من التقارير التي صدرت مؤخرا واحدا من أعقد الأدوات التي تم استخدامها إلى الآن.

حيث كان الخبراء يعتقدون أنّ مهمّة البرنامج هي التجسس الصناعي ونقل المعلومات التي تساعد على تقليد المنتجات، لكن تبيّن لخبراء الهندسة العكسيّة فيما بعد أنّ الأمر مختلف كليا فالبرنامج وعلى عكس الكثير من البرامج المعروفة إلى الآن ليس مخصصاً للتجسس وسرقة المعلومات الصناعية لمحاولة كسب المال أو لسرقة

الملكية الفكرية، فبعد حوالي أربعة أشهر من العمل، ظهر أن الأمر أكثر تعقيدا مما كان متصورا، وأننا نقف اليوم أمام نوع جديد من البرامج التي من الممكن أن تتحول إلى نموذج للأطراف التي

تنوي إطلاق هجمات إلكترونية تؤدي إلى دمار حقيقي وواقعي في البلد المستهدف حتى دون الحاجة إلى الإنترنت (https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out).

فالبرنامج لا يعمل بشكل عشوائي كما هي العادة وإنما بشكل محدد جدا، إذ يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة "سيمنز الألمانية"، فإذا ما وجدها يقوم عندها بتفعيل نفسه ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم وقد تتعدد المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط إلى محطات توليد الكهرباء وحتى المفاعلات النووية وغيرها من المنشآت الاستراتيجية الحسّاسة، أمّا إذا لم يجدها، فيترك الحاسوب وشأنه.

فالبرنامج كبير ومشفّر جدا ومعقد جدا ويوظّف تقنيات ذكية وجديدة، ولا يلزمه للعمل أي تدخل بشري في أي مرحلة من المراحل، ويكفي أن يكون هناك بطاقة ذاكرة تخزين إلكترونية مصابة به حتى يبدأ عمله.

ولأنه على هذه الدرجة من التعقيد والتطور ولأنّه يعمل بشكل محدد جدا، حيث يرى البعض أنه من صنع دولة، ومن البديهي أن تكون المنشأة أو المنشآت الأساسية التي يبحث عنها لتدميرها أو تخريبها قيّمة للغاية وعلى درجة عالية من الأهمية، وبناء على هذا الاستنتاج ذهبت العديد من المصادر إلى التخمين بأنّ مفاعل بوشهر الإيراني قد يكون الهدف الأساسي الذي يبحث البرنامج عنه لتدميره.

أشارت شركة "سيمناتيك" التي تعمل في مجال برامج الأمن الإلكتروني والبرامج المضادة للفيروسات أن إيران تأتي في طليعة الدول المستهدفة من ناحية الإصابات التي حققها برنامج "ستكسنت" وأن ما يقارب 60% من أجهزة الكمبيوتر التي تعرضت لهجوم من هذا التطبيق الخبيث كانت في إيران (شكر، 2019، ص. 11).

وعلى الرغم من أن إيران نفت عبر مدير مشروع بوشهر محمود جعفري أن يكون الفيروس قد أصاب المفاعل أو تسبب في أي ضرر في أنظمة التحكم فيه، إلا أنها كانت قد أقرت إصابة بعض الحواسيب الشخصية المحمولة لموظفي المحطة بهذا الفيروس إضافة إلى إصابته أكثر من 30 ألف نظام حاسوبي لمنشآت صناعية متعددة داخل إيران.

وهناك عدد من الخبراء يعتقد بالفعل أن هدف الفيروس الأساسي قد يكون مفاعل بوشهر، وأنّ الفيروس قد حقق هدفه من التخريب بدليل أن إيران أعلنت أنها ستؤجّل العمل في المفاعل عدّة أشهر حتى بداية عام 2011، ويرى فيه آخرون أنّ الهدف هو منشأة ناتانز لتخصيب اليورانيوم بدليل أنّ المنشأة عانت مشكلة ظلّت طي الكتمان وأدت إلى انخفاض أجهزة الطرد المركزية القادرة على العمل بنسبة 15% فجأة وذلك في نفس الفترة التي ظهر فيها الفيروس لأول مرّة.

2.5. الجهات المسؤولة عن الفيروس: والسؤال الذي يطرح نفسه هنا من هو المسؤول عن هذا الهجوم؟، ويمكن الاجابة على هذا السؤال من خلال التطرق إلى دراستين وهما:

أولا: لا تستبعد جهات أن تكون الولايات المتّحدة الدولة المصنّعة للفيروس نظرا لتعقيده وتطوره ولما يحتاجه من خبرات وموارد هائلة، ويربط البعض بين هذا الفيروس وبين النزاع الأمريكي-الإيراني حول الملف النووي، وأنّ الهدف منه هو تخريب المجهود النووي الإيراني خاصّة أنّ الرئيس الأسبق جورج بوش الابن كان قد سمح وفقا لتقارير صحفية نقلا عن مسؤولين حكوميين، بإطلاق جهود تتضمن العديد من الخطوات التي تهدف إلى تخريب البرنامج النووي الإيراني من خلال استهداف أنظمة الحواسيب والكهرباء والشبكات وكل ما يخدم البرنامج النووي الإيراني، ووفقا لأصحاب هذه الدراسة، فقد استكمل الرئيس السابق أوباما هذا المجهود فيما

بعد، خاصّة أنّ عملية تخصيب اليورانيوم كانت قد عانت مصاعب تقنية كبيرة عام 2010 وما زال من غير المعروف إذا ما كان السبب هو العقوبات الاقتصادية أم التصنيع الرديء أم عمليات التخريب الأمريكية.

ثانيا: تتجه أصابع الاتهام إلى إسرائيل دون الولايات المتحدة، فيما يتعلق بفيروس "ستكسنت" اعتمادا على عدد من المؤشرات منها: (https://www.reuters.com/article/us-israel-iran-cyberwar-analysis/wary-of-naked-force-israelis).

- توافر القدرات التقنية اللازمة للقيام بمثل ذلك العمل.
- تعقيدات العمل العسكري التقليدي والتردد الأمريكي في الدخول بحرب جديدة أو السماح لإسرائيل بفعل ذلك.
- توافر سوابق لإسرائيل في هذا المجال، لعل من أبرزها قصف إسرائيل عام 2007 لمفاعل نووي مزعوم في سوريا، كان مسبوقا بهجوم إلكتروني عطّل الرادارات الأرضية والراجمات المضادة للطيران.

كما يرى البعض وجود مؤشرات قوية تدلل على أن إسرائيل من قامت بهذا الهجوم وهي:

- في عام 2010 كشف رئيس شعبة المخابرات العسكرية الإسرائيلية "عاموس يادلين" في خطوة نادرة أن مجال الحرب الإلكترونية يناسب تماما عقيدة الدفاع في إسرائيل، وأنّ القوات الإسرائيلية أصبح لديها الوسائل الكافية لإطلاق هجمات إلكترونية استباقية من دون أي مساعدات خارجية، وهي تدرس بهدوء استخدام هذه التقنيات ضد الآخرين بهدف التسلل إلى معلومات أو القيام بتخريب من خلال زرع برامج في أنظمة السيطرة والتحكم في المنشآت الحساسة للأعداء في المنطقة مثل إيران. (شكر، ص. 13).
- كذلك في عام 2010 توصلت إسرائيل إلى أن نقطة ضعف إيران الكبرى إنما تكمن في معلوماتها المحملة إلكترونيا، وهو ما يتيح استهدافها، وعندما طرح سؤال على "سكوت بورج" مدير الوحدة الأمريكية لتبعات الإنترنت، وهي وحدة استشارية تقدم خدماتها في مجال الأمن الإلكتروني لمختلف الوكالات الأمنية الوطنية الأمريكية" عن السيناريو الذي يمكن أن تلجأ إليه إسرائيل لاستهداف إيران، أجاب أنه: من الممكن استخدام "البرامج الخبيثة" لإفساد أو إعطاب أو السيطرة على أجهزة التحكم في المواقع الحساسة مثل محطات تخصيب اليورانيوم، وبما أن الأصول النووية لإيران ستكون في الغالب غير متّصلة بالإنترنت، فلن يتسنى للإسرائيليين زرع الفيروس عبر الإنترنت وسيكون عليهم دسه في البرامج التي يستخدمها الإيرانيون أو في أجهزة محمولة يدخلها فنيون دون علم الإيرانيين، ويكفي توافر أي وحدة تخزين بيانات متنقلة ملوثة لإتمام هذه المهمة، وهو سيناريو شبيه بما حصل في إيران.
- أشار **"ليام أو مورشو"** وهو من الذين عملوا على تفكيك فيروس "ستكسنت"ودراسة وظيفته وقدم شرحا عمليا لقدرته التدميرية المادية من خلال تجربته على مضخّة إلى وجود كلمة مفتاحية في شفرة التعليمات الخاصة بالبرنامج تحمل كلمة(Myrtus)، وهي كلمة مرادفة باللغة العبرية لكلمة "ايستر" في إشارة إلى ملكة اليهود بفارس واسمها الحقيقي هاداسا التي أقنعت زوجها الملك الفارسي احشورش بالقضاء على كل من يعادي اليهود ومن بينهم أخلص وزرائه "هامان"، كما يقوم فيروس "ستكسنت" عندما يجد هدفه بعرض رقم من ثماني خانات (19790509)، وهو على الأرجح تاريخ 9 ماي 1979، ووفقا للأرشيف فإن هذا التاريخ شهد موت حبيب الغانيان، وهو أول إيراني يهودي تم إعدامه في إيران بعد الثورة الإسلامية بتهمة التجسس.

ويمكن القول إن إسرائيل هي المسؤول المباشر عن هذا الهجوم وبمساعدة الولايات المتحدة الأمريكية نظرا للإمكانية التقنية والتكنولوجية للبلدين وإلى حرصهما على إفشال المشروع النووي الإيراني لما يمثله من خطر محتمل لإسرائيل ولحرصها على أن تبقى البلد الوحيد الذي يملك السلاح النووي في المنطقة، إضافة إلى حرص الولايات المتحدة بأن لا تكون إيران دولة نووية.

3.5. تداعيات الهجمات الإلكترونية على إيران:

- تعرض إيران لمحاولة تخريب وإبطاء طموحاتها النووية.
- تعرض إيران لمشاكل فنية غير مفهومة خفضت عدد أجهزة الطرد المركزي العاملة ضمن برنامج تخصيب اليورانيوم.
- احتقان العلاقات الدبلوماسية الإيرانية الأمريكية، الإيرانية والإسرائيلية.
- الحاق أضرار بالوحدات الصناعية الإيرانية.
- هجوم ستكنست قدم نظرة مبكرة للشكل الذي ربما تتخذه المنازعات بين الدول في القرن الـ21.
- تزايد حدة النزاعات الإلكترونية بين الولايات المتحدة الأمريكية وإيران من جهة، ومن جهة أخرى بين إيران والسعودية بسبب الهجمات الأخيرة على منشآت النفط السعودية.

خاتمة:

من خلال العرض، نستنتج أن العصر الذى نعيش فيه بات عصرا رقميا تتحكم فيه المعرفة والمعلومات ووسائل الاتصالات، فمن يملك المعرفة يتحكم في كل شي، وأصبح الفضاء السيبراني واقع والحروب الإلكترونية حقيقة لا مفر منها والتي تعتبر الجيل الخامس من الحروب ويرى الكثير من الأكاديميين أنها نهاية الحروب فى المستقبل، وأصبحت الرقمنة هي الصياغة السائدة فى العصر الحالي من حكومات وسيادة سيبرانية وأمن سيبراني ودبلوماسية سيبرانية، كل شيء يتعامل عبر الفضاء الإلكترونى، ولذلك يتوجب على الدول والأفراد الحذر والحيطة عند استخدام البيانات والمعلومات فى المجال الافتراضي، لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز والجماعات الإرهابية.

أما ما يمكن استنتاجه من هذه الدراسة:

1- ليس هناك اتفاق واضح ومحدد فيما بين الباحثين حول مفهوم الحرب الإلكترونية شأنها شأن المفاهيم الأخرى.
2- اعتمدت الحروب التقليدية على المواجهة العسكرية المباشرة، بينما اعتمدت الحروب الإلكترونية على ثورة المعلومات والاتصالات في تنفيذ الهجمات وتحقيق أهدافها.
3- عدم اقتصار الحروب الإلكترونية على دولة دون أخرى، فقد أصبحت تداعيات الحروب الإلكترونية تتعدى الحدود الوطنية، وسيصبح لها التأثير الكبير على طبيعة العلاقات الدولية والسياسات العالمية، وذلك نتاجا لعدة عوامل: استخدام الهجمات الإلكترونية كأداة جديدة لتعزيز الدور الدولي، واستخدامها كمجال للصراع بين بعض الدول، وصعود أدوار الفاعلين من الدول الصغيرة والمتوسطة والفاعلين من غير الدول على الساحة الدولية، وحدوث توتر سياسي واحتقان دبلوماسي ينتج عن اتهام دولة لأخرى بالتدخل في شؤونها الداخلية عبر الفضاء الإلكتروني، وهذا ما حدث في نموذج الهجمات الإلكترونية على إيران.

ويمكن تقديم عدد من التوصيات المتعلقة بكيفية الحد من التأثيرات السلبية للحروب السيبرانية في النقاط التالية:

- العمل على المستوى الدولي في حل الصراعات الدولية، حيث إن ما يحدث في المجال الإلكتروني انعكس لحالة التوتر على الأرض، ومن ثم فإن خط المواجهة الأول يجب أن يكون العمل على حل وتسوية الصراعات بالطرق السلمية.
- العمل على تأمين البنية التحتية الكونية للمعلومات وإدخالها ضمن المنشآت المدنية المحظور استهدافها من قبل أطراف الصراع في حالة الحرب.
- قيام الدول على تحديث أطرها التشريعية لمكافحة الجريمة الإلكترونية لاحتواء المخاطر الداخلية على امن الفضاء الإلكتروني.
- إنشاء مراكز تدريب محلية في مجال مكافحة الجريمة الإلكترونية، وأهمية العمل على تعزيز التعاون في النظم القضائية وتبادل الخبرات.
- تعزيز التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وأهمية العمل على تعزيز التعاون في النظم القضائية وتبادل الخبرات.

قائمة المراجع:

أولا: قائمة المراجع باللغة العربية:

- **توثيق الكتب:**

1- أحمد، أشرف السعيد،(2013). القرصنة الإلكترونية، القاهرة: دار النهضة العربية.
2- بدران، عباس، (2010). الحرب الإلكترونية: الاشتباك في عالم المعلومات، بيروت: مركز دراسات الحكومة الإلكترونية.
3- جعفر، جاسم . (2010). حرب المعلومات بين إرث الماضي وديناميكية المستقبل، عمان: دار البداية للنشر والتوزيع.
4- زيتون، وضاح،(2006). المعجم السياسي ،عمان: دار اسامة للنشر والتوزيع.
5- شكر، عمر حامد. (2010). المجال الخامس- الفضاء الإلكتروني، القاهرة: المعهد المصري للدراسات.
6- عبد الصادق،عادل. (2016). الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق ، القاهرة: المكتبة الأكاديمية.
7- عبد الغفار، فيصل محمد، (2016). الحرب الإلكترونية، عمان: الجنادرية للنشر والتوزيع.
8- عياد، سامي، (2007). استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، القاهرة: دار الفكر الجامعي.
9- محمد البصيلي، رائد طيران جاسم، (1989). الحرب الإلكترونية أسسها وأثرها في الحروب، بيروت، المؤسسة العربية للدراسات والنشر.

- **الدوريات العلمية:**

1- بلفرد، لطفي لمين. (2016).الفضاء السيبراني: هندسة وفواعل، المجلة الجزائرية للدراسات السياسية. عدد.5. المدرسة الوطنية العليا للعلوم السياسية.
2- الزهراني، يحي مفرح. (شتاء 2017). الأبعاد الاستراتيجية والقانونية للحرب السيبرانية . مجلة البحوث والدراسات. عدد. 23.
3- عبد العزيز، سارة، (2017). التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية. اتجاهات الأحداث. عدد.20، الامارات العربية المتحدة.

4- عبد الوهاب، شادي، (2017). حروب الجيل الخامس: التحولات الرئيسية في المواجهات العنيفة غير التقليدية، دراسات المستقبل، عدد 1، الإمارات العربية المتحدة.
5- عبدالصادق، عادل، (أفريل 2012). القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني. مجلة السياسة الدولية.عدد 188، مركز الأهرام للدراسات السياسية والإستراتيجية.

- **الدراسات غير منشورة:**

1- جلعود، وليد غسان سعيد. (2013). دور الحرب الإلكترونية في الصراع العربي الإسرائيلي . أطروحة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية. كلية الدراسات العليا. جامعة النجاح الوطنية.فلسطين.
2- بريوش، نضال ناجي بدوي. (2018 -2019). الصراع السيبراني مع العدو الصهيوني . بحث مقدم لاستكمال دبلوم الدراسات الفلسطينية. أكاديمية دراسات اللاجئين. قسم الأبحاث والمشاريع.

- **المواقع الإلكترونية:**

1- عبد الصادق، عادل، الحرب السيبرانية وتداعياتها على الأمن العالمي، 23/ 06/ 2017، الموقع المختصر عبر http://alimbaratur.com/?p=2850 / ، 19/ 12/ 2019.
2- بن يحي،عمتد، دراسة الهجمات الإلكترونية كأكبر المخاطر التي تهدد قطاع الأعمال، 31/ 10/ 2012/، الموقع المختصر عبر https://www.tech-wd.com/wd/2012/09/08/kaspersky-global-it-security-risks-survey-report، 15/ 01/ 2020.

ثانيا: قائمة المراجع باللغة الأجنبية:

- **Books :**

1- Amstrom, Jan. (2005). introduction ; debating the nature of modern war, London : Frank class.
2- Dunnigan, James F. (2002). The Next War Zone: Confronting the Global Threat of Cyber terrorism, New York: Citadel Press.
3- Sanger, David E. (2012). Obama's Secret War and Surprising Use of American Power, New York: Crown.
4- Clarke, Richard A. Knake, Robert. (2010). Cyber War, The Next Threat to National Security and What to Do About It , New York: Harpercollins e-books.

- **Journals:**

1- Bieber, Florian, (2000). Cyber war or Sideshow The Internet and the Balkan Wars , Current History 99, n. 635.
2- Michael, Alex. (2010), Cyber Probing: The Politicisation of Virtual Attack. _Defence Academy of the United Kingdom.
3- Thomas Rid, (, November / December 2013). Cyberwar & Peace: Hacking Can Reduce Real World Violence, Foreign Affairs, Vol. 92, No. 6.
4- William J. Lynn. (2010). Defending a New Domain: The Pentagon's Cyber Strategy . Foreign Affairs.

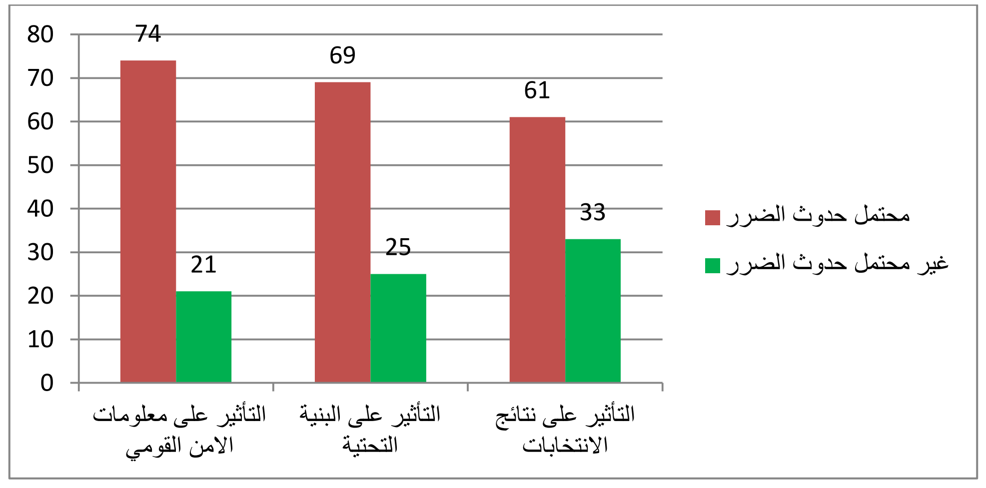
- **Electronic resources:**

1- Clayton, Mark, Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?, 21/ 09/ 2010, The short link is via https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant, 20/ 12/2019.

2- Williams, Dan, Wary of naked force, Israelis eye cyberwar on Iran, **07/ 07/2009/,** The short link is via https://www.reuters.com/article/us-israel-iran-cyberwar-analysis/wary-of-naked-force-israelis-eye-cyberwar-on-iran-idUSTRE5663EC20090707 20/12/2019.

ملاحق:

الشكل رقم (1): رأي الشعوب في تأثير الحروب الإلكترونية على الأمن القومي والبنية التحتية العامة والانتخابات



المصدر: Pew Research Center

الخريطة رقم (1) تمثل الدول الأعضاء في الدراسة



المصدر: **https://www.tech-wd.com/wd**